

## **Improved Method And System For Fingerprint Authentication**

### **Field of the Invention**

[001] This invention relates generally to imaging devices and more particularly to an improved method and system for reading and analyzing fingerprints.

### **Background of the Invention**

[002] Various optical devices are known which employ prisms upon which a finger whose print is to be identified is placed. The prism has a first surface upon which a finger is placed, a second surface disposed at an acute angle to the first surface through which the fingerprint is viewed and a third illumination surface through which light is directed into the prism. In some cases, the illumination surface is at an acute angle to the first surface, as seen for example, in US Patents 5,187,482 and 5,187,748. In other cases, the illumination surface is parallel to the first surface, as seen for example, in US Patents 5,109,427 and 5,233,404. Fingerprint identification devices of this nature are generally used to control the building-access or information-access of individuals to buildings, rooms, and devices such as computer terminals.

[003] One of the problems associated with fingerprint sensors concerns the reliable and accurate transformation of the ridge-and-valley pattern of the fingertip into electrical or optical signals to be stored in a digital format. Optical systems as described above, for example using a prism, require sophisticated equipment and tend to be bulky and costly.

[004] In an attempt to overcome some of the limitations and disadvantages of using optical systems based on illumination of the finger tip, United States patent number 4,353,056 in the name of Tsikos issued October 5, 1982, discloses an alternative kind of fingerprint sensor that uses a capacitive sensing approach. The described sensor has a two dimensional, row and column, array of capacitors, each comprising a pair of spaced electrodes, carried in a sensing member and covered by an insulating film. The sensors rely upon deformation to the sensing member caused by a finger being placed thereon so as to vary locally the spacing between capacitor electrodes, according to the ridge-and-valley pattern of the

fingerprint, and hence, the capacitance of the capacitors. In one arrangement, the capacitors of each column are connected in series with the columns of capacitors connected in parallel and a voltage is applied across the columns. In another arrangement, a voltage is applied to each individual capacitor in the array. Sensing in the respective two arrangements is accomplished by detecting the change of voltage distribution in the series connected capacitors or by measuring the voltage values of the individual capacitances resulting from local deformation. To achieve this, an individual connection is required from the detection circuit to each capacitor.

[005] While the described sensor may not suffer from the problems associated with the kind of sensor employing an optical sensing technique, it suffers from its own problems. For example, applying a voltage to the array of capacitors requires circuitry to each capacitor for charging. Such charging also requires further states in the imaging process consuming more resources and providing added areas for unreliability. Moreover, the need to provide a respective connection to each individual capacitor in the array means that a very large number of connecting lines is necessary. This creates difficulties, both in the fabrication of the sensing member and its interconnection with the detection circuit.

[006] In yet another attempt to improve upon deficiencies and limitations of the aforementioned and other prior art, a further contact imaging device is described in United States patent number 5,325,442 in the name of Knapp, issued June 28, 1994. Those parts of the disclosure of this patent not included in this specification are incorporated herein by reference.

[007] Knapp describes making a capacitance measuring imaging device in the form of a single large active matrix array involving deposition and definition by photolithographic processes of a number of layers on a single large insulating substrate. Electrodes and sets of address conductors formed of metal and field effect transistors are formed as amorphous silicon or polycrystalline silicon thin film transistors (TFTs) using an appropriate substrate of, for example, glass or quartz.

[008] A fingerprint sensing device and recognition system that includes an array of closely spaced apart sensing elements each comprising a sensing electrode and an

amplifier circuit is described in United States patent number 5,778,089 in the name of Borza, issued July 7, 1998. The device is used to sense electrical charge on a fingertip and obviates the need to pre-charge the sensing electrode. The device may be constructed with a single die or with multiple dies. Those parts of the disclosure of this patent not included in this specification are incorporated herein by reference.

[009] Fingerprint analysis is perhaps the most widely used and studied biometric technique. The analysis of fingerprints is discussed in the following references which are hereby incorporated by reference:

Xiao Qinghan and Bian Zhaoqi,: An approach to Fingerprint Identification By Using the Attributes of Feature Lines of Fingerprint,” IEEE Pattern Recognition, pp 663, 1986;

C.B. Shelman, “ Fingerprint Classification - Theory and Application,” Proc. 76 Carnahan Conference on Electronic Crime Countermeasures, 1976;

Feri Pernus, Stanko Kovacic, and Ludvik Gyergyek, “Minutiae Based Fingerprint Registration,” IEEE Pattern Recognition, pp 1380, 1980;

J.A. Ratkovic, F.W. Blackwell, and H.H. Bailey, “Concepts for a Next Generation Automated Fingerprint System,” Proc. 78 Carnahan Conference on Electronic Crime Countermeasures, 1978;

K. Millard, “ An approach to the Automatic Retrieval of Latent Fingerprints,” Proc. 75 Carnahan Conference on Electronic Crime Countermeasures, 1975;

Wegstein, *An Automated Fingerprint Identification System*, NBS special publication, U.S. Department of Commerce/National Bureau of Standards, ISSN 0083-1883; no. 500-89, 1982; and

Moenssens, Andre A., *Fingerprint Techniques*, Chilton Book Co., 1971; and,

Wegstein and J.F. Rafferty, *The LX39 Latent Fingerprint Matcher*, NBS special publication, U.S. Department of Commerce/National Bureau of Standards; no. 500-36, 1978.

[0010] Typically in electronic fingerprint matching, a live fingerprint is scanned and electronically digitized. The digitized data generally contains information pertaining to

characteristic features of the fingerprint, such as ridge endings, points of ridge bifurcation, and the core of a whorl i.e., fingerprint minutiae. The digitized data is then compared with stored data relating to fingerprints that have been obtained previously from corresponding authorized persons i.e., fingerprint templates. When a match is detected, within a predetermined level of security in the form of a predetermined false acceptance rate, the individual is identified and a corresponding action is performed.

[0011] In general, there are two types of errors associated with fingerprint identification. The first is false reject (Type I) error and the second is false accept (Type II) error. False accept errors occur when there are enough similarities between fingerprints of two individuals, that one is mistaken for the other. A false reject error occurs for a variety of reasons, and refers to when an individual is not identified even though the individual is an authorized user registered with the system.

[0012] A moisture dependent variation of the ridge-and-valley pattern of a same fingertip often leads to an increased incidence of Type I errors, which causes undue inconvenience to users of a fingerprint identification system. For instance, seasonal weather patterns, high levels of physical exertion, the user wearing gloves to warm his hands, etc. can cause a fingertip to be excessively dry or excessively moist relative to a template fingerprint that was provided during an initial enrollment operation. A warm, moist fingertip tends to be swollen slightly, such that adjacent ridges are pushed more closely together and may connect (a ridge inter-connect). Further, the fingerprint identification system may mistakenly register sweat or moisture that is trapped within a valley as a fingertip ridge. In contrast, a cool, dry fingertip tends to be constricted slightly, such that portions thereof fail to make proper contact with the imaging surface, causing the fingerprint identification system to register gaps or discontinuities where there is in fact a continuous ridge. Of course, when a sample image from one of a moist and a dry fingertip is compared to a reference image obtained previously under ideal conditions, there is an increased likelihood that the user will be falsely rejected.

[0013] U.S. Patent 6,241,288, issued June 5, 2001 to Bergenek et al., teaches a fingerprint identification/verification method using stored bitmap images of a reference

fingerprint to correlate with a bitmap image of an input fingerprint. The method includes a user enrollment step, during which step an imaging device captures a binarized reference image of a fingerprint presented by the user. The binarized reference image is checked for 'dryness' or 'wetness' as part of a quality control portion of the enrollment step. If the image is 'too dry', the pressure applied to the sensor was too light or the sensor failed to detect parts of ridges because of fingertip dryness. If the image is 'too wet', moisture on the fingertip 'flooded' the fingerprint valleys. Wetness or dryness is detected by analyzing the image for too few dark pixels (dryness) or, too many dark pixels and continuous dark areas (wetness). If the reference image is rejected, the person is asked to correct the problem and another reference image is taken. Optionally, the input fingerprint is subjected to a similar quality control process during a recognition step of the method, for instance when the user wishes to be authenticated. Unfortunately, the onus is on the user to correct the problem, causing the user to suffer inconvenience unnecessarily.

[0014] U.S. Patent 6,131,464, issued October 17, 2000 to Pare, Jr. et al., discloses a pressure sensitive biometric input apparatus and a method of operating same. An image of a fingertip under investigation is captured at an imaging area of the apparatus. If the image is too dark, the pressure at which the image was scanned is examined. If the pressure is at the higher end of a predetermined pressure range, a preferred embodiment of the invention instructs the user to use less pressure, postulating that the user might have well-defined ridges and a decrease in pressure might well lighten the image to an acceptable level. Otherwise, an embodiment of the invention concludes that the most likely cause of the problem is too much moisture, and instructs the user to dry his or her finger and retry the scan. Unfortunately, the user must attempt multiple fingerprint scans before an acceptable match is obtained. Further unfortunately, the onus is on the user to correct the problem, causing the user to suffer inconvenience unnecessarily.

[0015] It would be advantageous to provide a method and a system to process data indicative of a fingerprint image and to determine a value in dependence upon a moisture level thereof, prior to attempting user authentication. The determined value for selecting

a particular reference fingerprint of a plurality of reference fingerprints, each of the plurality of reference fingerprints obtained at a known fingertip moisture state.

### **Object of the Invention**

[0016] Thus, in an attempt to overcome these and other limitations of known prior art devices, it is an object of this invention to provide a method of biometric identification that is robust.

[0017] It is a further object of the invention to provide a method of detecting a characteristic of a biometric surface for use in identification of an individual.

### **Summary of the Invention**

[0018] In accordance with the present invention there is provided a method for fingerprint authentication comprising the steps of:

- a) acquiring an image of a fingertip;
- b) processing the image to determine a value indicative of a predetermined acquisition parameter thereof;
- c) comparing the image to a stored biometric template, the comparison process based on the determined value; and,
- d) performing one of an authentication and a rejection in dependence upon the comparison.

[0019] In accordance with the present invention there is provided another method for processing a fingerprint image comprising the steps of:

- a) acquiring an image of a fingertip;
- b) processing the acquired image to determine a value indicative of a predetermined acquisition parameter thereof; and,
- c) selecting an image-processing process in dependence upon the determined value, the image-processing process for removing a subset of features of the acquired image.

[0020] In accordance with the present invention there is provided yet another method for fingerprint authentication comprising the steps of:

- a) acquiring an image of a fingertip;
- b) processing the acquired image to determine a value indicative of a predetermined acquisition parameter thereof;
- c) processing the acquired image according to a predetermined image-processing process to remove a subset of features from the acquired image;
- d) selecting a biometric template in dependence upon the determined value, the biometric template processed according to the predetermined image-processing process;
- e) comparing the processed acquired image to the biometric template; and,
- f) performing one of an authentication and a rejection in dependence upon the comparison.

[0021] In accordance with the present invention there is provided a system for fingerprint authentication comprising:

- a sensing area for capturing an image of a fingertip presented thereto;
- a memory storage area for storing captured images therein; and,
- a processor for executing code thereon to process the captured image to determine a value indicative of an acquisition parameter thereof, and to compare the captured image to a template image according to an image-processing process selected in dependence upon the determined value.

### **Brief Description of the Drawings**

[0022] Exemplary embodiments of the invention will now be described in conjunction with the following drawings, in which similar reference numbers designate similar items:

[0023] Fig. 1 is a simplified diagram of a prior art sensing device showing an array of sensing elements together with associated addressing circuitry, the size of the sensing device surface is consistent with the size of the surface to be sensed;

[0024] Fig. 2 is a simplified diagram of a prior art sensing element;

[0025] Fig. 3 is a schematic diagram of an amplifier circuit in the form of a differential amplifier for use with the prior art sensing element;

[0026] Fig. 4a is a schematic diagram of an alternative amplifier circuit in the form of a differential amplifier for use with the prior art sensing element;

[0027] Fig. 4b is a schematic diagram of an alternative amplifier circuit for use with the prior art sensing element;

[0028] Fig. 5a is a schematic illustration of a 'dry' fingerprint image having numerous ridge discontinuities;

[0029] Fig. 5b is a schematic illustration of a 'normal' fingerprint image having a few ridge discontinuities and a few ridge interconnections;

[0030] Fig. 5c is a schematic illustration of a 'moist' fingerprint image having numerous ridge interconnections;

[0031] Fig. 6 is a simplified block diagram of a fingerprint identification/verification system according to the instant invention;

[0032] Fig. 7a is a simplified flow diagram of an enrollment operation for use with the fingerprint identification/verification system according to a first preferred embodiment of the instant invention;

[0033] Fig. 7b is a simplified flow diagram of an enrollment operation for use with the fingerprint identification/verification system according to a second preferred embodiment of the instant invention;

[0034] Fig. 7c is a simplified flow diagram of an enrollment operation for use with the fingerprint identification/verification system according to a third preferred embodiment of the instant invention;

[0035] Fig. 7d is a simplified flow diagram of an enrollment operation for use with the fingerprint identification/verification system according to a fourth preferred embodiment of the instant invention;

[0036] Fig. 8 is a simplified flow diagram of an authentication process for use with the fingerprint identification/verification system according to an embodiment of the instant invention;

[0037] Fig. 9 is a simplified flow diagram of another authentication process for use with the fingerprint identification/verification system according to an embodiment of the instant invention;



[0038] Fig. 10 is a simplified flow diagram of yet another authentication process for use with the fingerprint identification/verification system according to an embodiment of the instant invention.

### Detailed Description of the Invention

[0039] A prior art sensing device that is suitable for use with the instant invention comprises a substantially flat surface for receiving a fingertip. Below the surface are a sensor array and a measuring array. The arrays comprise sensing elements that are designed to sense induced electrical charge. The distance between the fingertip and individual sensing elements should generally be kept to a very small gap in order to retain a high signal to noise ratio. Optionally, the surface for receiving the fingertip is curved, such as for instance a rotatably mounted cylindrical roller for sensing a fingertip swiped in a direction transverse to a longitudinal axis thereof. Further optionally the surface for receiving the fingertip comprises a plurality of separate sensor arrays.

[0040] Referring to Fig. 1, part of a prior art sensing device for use with the present invention is shown. The device comprises a single active matrix addressed sensing pad 19 having an X-Y array of sense elements having r rows (1 to r) each having c sensing elements 17. In practice there are about 300 rows and 200 columns of regularly spaced elements 17 occupying an area of approximately 2 cm x 3 cm. This area is for accepting a fingertip for scanning.

[0041] Preferably sensing elements 17 are disposed in such a fashion that a smallest desired feature of a fingerprint is evident in the sensed data. The placement and spacing of the sensor elements allows an image of a fingerprint, once scanned, to contain all required features for analysis. A sensing element 17 is preferably smaller than half the smallest sensible feature size in order to generate such an image. Empirical studies have shown that a square plate of about 50  $\mu\text{m}$  edge length is suitable for fingerprint sensing.

[0042] The array of sensing elements 17 is connected through an analog switch matrix to facilitate reading the fingerprint image out of the sensing pad 19. Timing and sequencing logic 16 selects each element in the array, in turn, to produce a complete image of a

fingerprint presented to the device. The signal is output directly as an analog signal or, alternatively, is converted to a digital signal prior to output from the device.

[0043] The sensing pad **19** further comprises a ground ring **15** and bonding pads **18** designed for connection to other components or to packaging. The ground ring **15** also serves to provide a common ground for the sensing pad. In this role, it is important that the ground ring **15** and integrated circuit elements be designed so as to minimize noise to each sensing element **17**. The signal to noise ratio that is acceptable varies between applications and should be adjusted to meet the needs of a specific design. When possible, packaging should be selected to limit noise.

[0044] Referring to Fig. 2, a prior art single sensing plate **20** is shown. Such a sensing plate **20** is designed for use in arrays and is smaller than half the smallest sensible feature size as indicated above. Charge sensing electrode **21** is connected to an active element, shown as a three terminal switching device in the form of a field effect transistor (FET) having a source, a drain, and a gate **26**. The gate **26** is connected to the sensing electrode **21** by an interconnect **24**. Disposed between the gate **26** and the transistor **30** is a gate oxide **27**.

[0045] Above the charge sensing electrode **21** is disposed an overglass **22** which serves to protect the charge sensing electrode **21** and to space the electrode and a fingertip presented thereto. Below the charge sensing electrode **21** is disposed a field oxide **25**. A finger placed against the overglass **22** induces charge in the charge sensing electrode **21**. The charge so induced is greater for portions of the fingertip that are in contact with the overglass **22** - ridges - than for those portions of the fingertip spaced from the overglass **22** - valleys. By amplifying the charges so induced with an amplifier circuit such as is shown in Fig. 3, the induced charges are rendered easily distinguishable.

[0046] Assuming that the charge density on the fingertip is substantially even, induced charges on the charge sensing electrode **21** depend solely on the distance between the charge sensing electrode **21** and the skin of the fingertip inducing the charge. Further, as the induced charge falls off with the distance, the closest skin of the fingertip will induce a larger proportion of the charge.

[0047] Referring to Fig. 3, an amplifier circuit for use with the instant invention is disclosed. Other suitable amplifier circuits may also be used. A distributed diode resistor network 31 is used to protect the amplifier circuit from electrostatic discharge. A low pass filter network 32, shown as a combination of two resistors and a capacitor stabilizes the DC operating point without impacting AC gain of the amplifier circuit. Any low pass filter circuit with similar characteristics may be employed. The cutoff frequency of the filter is set well below 1Hz to keep gain high for slowly varying signals.

[0048] Capacitor 33 having a capacitance of  $C_f$  provides feedback necessary to convert the input charge to a proportional voltage. Sensitivity of the amplifier in its passband is set by the choice of  $C_f$  as  $V_o = Q_i / C_f$ , where  $Q_i$  is the input charge at sense electrode 20. For example, at  $C_f = 0.2 \text{ pF}$ , sensitivity of approximately 5 V/pC is achieved. In practice, the capacitance of the input transistor 34 and protection network 31 attenuates the signal, which affects the final design gain of the amplifier and choice of feedback capacitance  $C_f$ . Thus, it is suggested that some tuning of the circuit be performed during design.

[0049] Amplifiers 35 and 36 and associated circuitry provides level shifting and additional voltage gain. Output signals from the amplifier 36 are selectively switched by on-chip sequential control logic similar to that used in solid state serial memory devices to produce a serialized stream of output signals corresponding to an output of each sensing element 20 at discrete points in time. Alternatively, the output signal from the amplifier is switched by random access logic as is used in random access memory devices and then digitized. The order of the switching and the digitizing may be reversed but so doing requires more logic and is thus more costly.

[0050] Two alternative embodiments for the amplifier circuit are shown in Fig. 4. Fig. 4a shows a true differential amplifier. Though similar to the amplifier circuit of Fig. 3, the transistor 37 is connected to at least an adjacent sensing element 20a. In practice, such a differential amplifier circuit reduces common mode voltages thereby increasing resolution. In Fig. 3, the transistor 37 is connected to ground providing a virtual reference of ground. Thus the circuit of Fig. 3 measures all induced voltages relative to a ground including any common mode voltage induced. Preferably, the ground is a

common ground in the form of the ground ring **15**. When using the circuit of Fig. 4a with multiple adjacent sensing elements used as a reference, complexity is introduced to the amplifier and potentially added cost.

**[0051]** Fig. 4b shows another alternative embodiment for the amplifier circuit. This circuit is very simple and similar to amplification of a current source. By treating the induced charge on the sensing elements as a current source, the number of transistors required is minimized and the yield is effectively increased. The overall circuit comprises electrostatic protection circuitry **31**, a low pass filter **32**, and an amplifier circuit.

**[0052]** In use the differential amplifier circuit obviates a need to apply a predetermined initial charge to a sensing electrode. Avoiding the initial charging of the sensing electrode simplifies the overall circuit and removes some sources of noise caused by added circuitry necessary for accomplishing the initial charging.

**[0053]** Referring to Fig. 5a-c, shown are exemplary 'dry', 'normal' and 'moist' fingerprint images, respectively. As will be obvious to one of skill in the art, features of a fingerprint vary in dependence upon acquisition parameters thereof, such as for instance the moisture condition of the fingertip. For instance, a 'dry' fingerprint as is shown in Fig. 5a typically includes relatively more ridge discontinuities compared to a 'moist' fingerprint as is shown in Fig. 5c. An image-processing process according to the prior art typically removes all incidences of ridge discontinuities – typically indicative of dryness – and ridge interconnects – typically indicative of excess moisture. Unfortunately, at least some of said removed features typically are real features of the fingerprint, for instance the normal fingerprint shown in Fig. 5b includes incidences of ridge discontinuities and ridge interconnects. As such, the prior art method when applied to fingerprint image templates results in stored templates containing only a minimum set of features for comparison to a fingerprint presented for authentication thereof. It is a limitation of the prior art methods that user authentication is based on a sub-set of fingerprint – features such as minutiae, and as such the level of security, reliability, and ease of use provided by a system employing the prior art methods is less than optimal. Of course, acquisition

parameter has been described in the form of a moisture content of a fingertip in the above example. More broadly, however, the term acquisition parameter relates to a global parameter relating to a condition of a biometric sample during sensing thereof. These include a sore throat for voice recognition systems, presence of a contact lens for retinal scan systems, and so forth. They also include, in some embodiments, portions of an image well captured. For example, too much pressure may be exerted on the right side of a palm print and too little pressure on the left side. Examples of acquisition parameters are pressure, moisture, dirt, damage, and so forth

[0054] Referring to Fig. 6, shown is a simplified block diagram of a fingerprint identification/verification system **50** according to the instant invention. A fingerprint scanner **53** comprises a sensing area **52** for receiving a fingertip **51** of a user wishing to be authenticated. The fingerprint scanner **53** is one of an electronic fingerprint scanner, such as for instance the capacitive sensing array described with reference to Figs. 1 and 2, and an optical fingerprint scanner employing a prism. Optionally, other types of fingerprint scanners that are well known in the art are employed. In operation, the fingerprint scanner **53** is in electrical communication with a processor **54** having software code in execution thereon for processing data indicative of a sensed fingerprint. The processor **54** is in electrical communication with a memory storage device **55**. In a preferred embodiment the memory storage device **55** includes a first memory area **55a** and a second memory area **55b**, for instance the first memory area **55a** comprises non-volatile memory and the second memory area **55b** comprises volatile memory. The non-volatile memory **55a** is for storing template images and/or image-processing processes that are for execution on processor **54**. Optionally, the fingerprint scanner **53** is in electrical communication with the second addressable area **55b** of the memory storage device **55**. Further optionally, the system **50** includes an output display device (not shown) in communication with the processor **54** for providing prompts, signals and/or authentication results to at least one of a user and an administrator of the system **50**.

[0055] Prior to using the system **50** for authentication purposes, each user enrolls with the system according to a predetermined enrollment process. Referring to Fig. 7a, shown is a simplified flow diagram of an enrollment process for use with a first preferred

embodiment of the instant invention. The user accesses an enrollment function of the system at step **100**, for instance the user provides a user name and password to log on to a computer system (not shown) in communication with the processor **54**. In a preferred embodiment there is provided biographic information and security information to be stored in an enrollment file. Optionally, the provided information is entered by one of the user, a system administrator supervising and/or monitoring the user enrollment process, and a secure token containing previously authenticated enrollment information.

[0056] At step **101** the user conditions a fingertip to be, for example, in a 'normal' moisture level condition. Optionally, the fingertip is assumed to be in a 'normal' moisture level condition and step **101** is not performed. Of course, a 'normal' moisture level condition is considered to be a range of fingertip conditions that is approximately central to conditions of extreme dryness and of extreme moistness. In a preferred embodiment of the instant invention, a carrier (not shown) of a skin-conditioning agent such as one of a porous pad and a roller is contacted by the fingertip **51** to moisten the fingertip. A blotter (not shown) is provided to remove excess skin-conditioning agent from the fingertip **51** placed in contact therewith, leaving the fingertip in a condition within the 'normal' moisture level range. The fingertip **51** that is conditioned is one of a predetermined fingertip, such as a right thumb, a user selected fingertip or a fingertip selected by the system. Optionally, a plurality of different fingertips is conditioned.

[0057] The user at step **102** places the conditioned finger onto the sensing area **52** of the fingerprint scanner **53**. At step **103** the image of the conditioned finger is captured, and at step **104** the captured image is stored in the first memory area **55a**. Optionally, the processor **54** performs post-capture image processing or editing prior to storing the captured image in the first memory area **55a**.

[0058] At step **105** the fingertip **51** is conditioned to be for example, in a 'dry' moisture level condition. Of course, a 'dry' moisture level condition is considered to be a range of fingertip conditions wherein the fingertip carries substantially less moisture than is 'normal'. In a preferred embodiment of the instant invention, one of a warm air blower (not shown), a blotter (not shown) and a carrier of a desiccating agent (not shown) is

provided to excess remove moisture from the fingertip **51**, leaving the fingertip in a 'dry' condition. The user at step **106** places the conditioned finger onto the sensing area **52** of the fingerprint scanner **53**. At step **107** the image of the conditioned finger is captured, and at step **108** the captured image is stored in the first memory area **55a**. Optionally, the processor **54** performs post-capture image processing or editing, for instance removes ridge discontinuities, prior to storing the captured image in the first memory area **55a**.

[0059] At step **109** the fingertip **51** is conditioned to be for example, in a 'moist' moisture level condition. Of course, a 'moist' moisture level condition is considered to be a range of fingertip conditions wherein the fingertip carries substantially more moisture than is 'normal'. In a preferred embodiment of the instant invention, a carrier (not shown) of a skin-conditioning agent such as one of a porous pad and a roller is contacted by the fingertip **51** to moisten the fingertip. The user at step **110** places the conditioned finger onto the sensing area **52** of the fingerprint scanner **53**. At step **111** the image of the conditioned finger is captured, and at step **112** the captured image is stored in the first memory area **55a**. Optionally, the processor **54** performs post-capture image processing or editing, for instance ridge interconnects, prior to storing the captured image in the first memory area **55a**.

[0060] The enrollment process of Fig. 7a terminates at step **113**.

[0061] Referring to Fig. 7b, another embodiment of the invention is shown in flow diagram. The user accesses an enrollment function of the system at step **100**, for instance the user provides a user name and password to log on to a computer system (not shown) in communication with the processor **54**. In a preferred embodiment there is provided biographic information and security level information to be stored in an enrollment file. Optionally, the provided information is entered by one of the user, a system administrator supervising and/or monitoring the user enrollment process, and a secure token containing previously authenticated enrollment information.

[0062] At step **101** the user conditions a fingertip to be in a 'normal' moisture level condition. Optionally, the fingertip is assumed to be in a 'normal' moisture level condition and step **101** is not performed. The user at step **102** places the conditioned

finger onto the sensing area **52** of the fingerprint scanner **53**. At step **103** the image of the conditioned finger is captured. Here, a single normal fingertip is imaged wherein normal denotes a level of moisture content approximately midway between extremes of dry and moist. The image captured is characterized at step **125** to extract therefrom a fingerprint template for use in user identification. The 'normal' template is stored at step **126** in association with a normal moisture level. This is similar to prior art template generation processes though here it is important that the user's fingertip be at a known normal moisture level.

[0063] The same fingerprint image is then characterized again at step **127** as if it were dry. This results in the removal of any features within the image that are possibly caused by dryness of the fingertip such as ridges that have breaks therein. The resulting template is based on a subset of features within the image and, as such, differs from the normal template. The features that are removed in the characterization process will be removed during fingerprint clean-up performed later should a fingertip be deemed dry during processing of an image thereof. Therefore, these features are necessarily removed. The 'dry' template is stored at step **128** in association with a dry moisture level.

[0064] Similarly, the same fingerprint image is then characterized again at step **129** as if it were moist. This results in the removal of any features within the image that are possibly caused by moisture of the fingertip such as ridges that have connections therebetween. The resulting 'moist' template is based on a subset of features within the image and, as such, differs from the 'normal' template. The features that are removed in the characterization process will be removed during fingerprint clean-up performed later should a fingertip be deemed moist during processing of an image thereof. Therefore, these features are necessarily removed. The 'moist' template is stored at step **130** in association with a moist moisture level.

[0065] As such, three templates result from a single image each based on a different state of an imaged fingertip. One of skill in the art will appreciate that in the 'moist' fingerprint template, features indicative of dryness and not of moistness remain. Similarly in the 'dry' fingerprint template, features indicative of moisture and not of



dryness remain. Thus, a largest possible subset of reliable features remains for each template.

[0066] The enrollment process of Fig. 7b terminates at step **113**.

[0067] Referring to Fig. 7c, shown is a simplified flow diagram of an enrollment process for use with a second preferred embodiment of the instant invention. The user accesses an enrollment function of the system at step **100**, for instance the user provides a user name and password to log on to a computer system (not shown) in communication with the processor **54**. In a preferred embodiment there is provided biographic information and security level information to be stored in an enrollment file. Optionally, the provided information is entered by one of the user, a system administrator supervising and/or monitoring the user enrollment process, and a secure token containing previously authenticated information.

[0068] The user at step **114** places a fingertip onto the sensing area **52** of the fingerprint scanner **53**. In response to a prompt from the system **50**, the user applies an indicated first amount of pressure to the sensing area **52** via fingertip **51**, for instance a 'normal pressure'. In a preferred embodiment, the sensing area **52** includes a pressure sensor for providing a feedback signal to instruct the user to apply one of increased or decreased first amount of pressure. Optionally, the user determines subjectively the first amount of pressure that is 'normal'. At step **115** the 'normal pressure' image of the finger is captured, and at step **116** the captured 'normal pressure' image is stored in the first memory area **55a**. Optionally, the processor **54** performs post-capture image processing or editing prior to storing the captured 'normal pressure' image in the first memory area **55a**.

[0069] In response to another prompt from the system **50**, the user at step **117** applies an indicated second amount of pressure to the sensing area **52** via fingertip **51**, for instance a 'light pressure'. In a preferred embodiment, the sensing area **52** includes a pressure sensor for providing a feedback signal to instruct the user to apply one of increased or decreased second amount of pressure. Optionally, the user determines subjectively the second amount of pressure that is 'light'. At step **118** the 'light pressure' image of the

finger is captured, and at step 119 the captured 'light pressure' image is stored in the first memory area 55a. Optionally, the processor 54 performs post-capture image processing or editing prior to storing the captured 'light pressure' image in the first memory area 55a.

[0070] In response to yet another prompt from the system 50, the user at step 120 applies an indicated third amount of pressure to the sensing area 52 via fingertip 51, for instance a 'heavy pressure'. In a preferred embodiment, the sensing area 52 includes a pressure sensor for providing a feedback signal to instruct the user to apply one of increased or decreased third amount of pressure. Optionally, the user determines subjectively the third amount of pressure that is 'heavy'. At step 121 the 'heavy pressure' image of the finger is captured, and at step 122 the captured 'heavy pressure' image is stored in the first memory area 55a. Optionally, the processor 54 performs post-capture image processing or editing prior to storing the captured 'heavy pressure' image in the first memory area 55a.

[0071] The enrollment process of Fig. 7c terminates at step 113.

[0072] Referring to Fig. 7d, another embodiment of the invention is shown in flow diagram. The user accesses an enrollment function of the system at step 100, for instance the user provides a user name and password to log on to a computer system (not shown) in communication with the processor 54. In a preferred embodiment there is provided biographic information and security level information to be stored in an enrollment file. Optionally, the provided information is entered by one of the user, a system administrator supervising and/or monitoring the user enrollment process, and a secure token containing previously authenticated enrollment information.

[0073] The user at step 114 places a fingertip onto the sensing area 52 of the fingerprint scanner 53. In response to a prompt from the system 50, the user applies an indicated first amount of pressure to the sensing area 52 via fingertip 51, for instance a 'normal pressure'. In a preferred embodiment, the sensing area 52 includes a pressure sensor for providing a feedback signal to instruct the user to apply one of increased or decreased first amount of pressure. Optionally, the user determines subjectively the first amount of

pressure that is 'normal'. At step **115** an image of the finger is captured. The image captured is characterized at step **131** to extract therefrom a fingerprint template for use in user identification. The 'normal' pressure template is stored at step **132** in association with a 'normal' applied pressure level. This is similar to prior art template generation processes though here it is important that the user's fingertip be at a known 'normal' applied pressure level.

[0074] The same fingerprint image is then characterized again at step **133** as if it were obtained when the user applied inadequate or 'light' pressure. This results in the removal of any features within the image that are possibly caused by a failure of the user to press the fingertip firmly against the sensing area **52** of the scanner **53**, such as for instance ridges that have breaks therein. The resulting template is based on a subset of features within the image and, as such, differs from the 'normal' pressure template. The features that are removed in the characterization process will be removed during fingerprint clean-up performed later should a fingertip pressure be deemed 'light' during processing of an image thereof. Therefore, these features are necessarily removed. The 'light' pressure template is stored at step **134** in association with a 'light' applied pressure level.

[0075] Similarly, the same fingerprint image is then characterized again at step **135** as if it were obtained when the user applied excessive or 'heavy' pressure. This results in the removal of any features within the image that are possibly caused by the user pressing the fingertip excessively hard against the sensing area **52** of the scanner **53**, such as for instance ridges that have connections therebetween. The resulting template is based on a subset of features within the image and, as such, differs from the 'normal' pressure template. The features that are removed in the characterization process will be removed during fingerprint clean-up performed later should a fingertip pressure be deemed 'heavy' during processing of an image thereof. Therefore, these features are necessarily removed. The 'heavy' pressure template is stored at step **134** in association with a 'heavy' applied pressure level.

[0076] As such, three templates result from a single image each based on a different applied pressure of an imaged fingertip. One of skill in the art will appreciate that in the

‘heavy’ fingerprint template, features indicative of excessive applied pressure and not of insufficient applied pressure remain. Similarly in the ‘light’ fingertip template, features indicative of insufficient applied pressure and not of excessive applied pressure remain. Thus, a largest possible subset of reliable features remains for each template.

[0077] The enrollment process of Fig. 7d terminates at step 113.

[0078] Optionally, the user enrolls according to at least two of the methods described with reference to Figs. 7a-7d, for instance the user enrollment file includes a plurality of template images obtained for a range of fingertip moisture levels and a plurality of template images obtained for a range of fingertip pressures. Further optionally, each plurality of template images includes more than three template images. For instance, a plurality of template images includes images obtained for very dry, dry, normal, moist and very moist levels of the fingertip 51. Still further optionally, the enrollment process of at least one of Fig. 7a, 7b 7c and 7d is repeated using at least a second different fingertip of the user.

[0079] In an alternate embodiment, the user provides a single template image during the enrollment process and subsequently, for instance during use, the system 50 ‘learns’ gradually to identify images of ‘moist’ and ‘dry’ fingerprints. In one embodiment, the template image is updated at predetermined intervals using, for example, a last fingerprint image provided by the user and resulting in authentication thereof. Of course, the fingerprint image is processed to remove ridge discontinuities and/or ridge interconnects, which often are transient features of a fingerprint and vary in dependence upon the level of moisture carried upon the fingertip being imaged. Some ridge discontinuities and/or ridge interconnects, after being detected consistently over a predetermined period of time, may in fact represent actual permanent or semi-permanent features of the fingerprint and as such can be added to the template image the next time it is updated or, preferably, over time in a gradual fashion.

[0080] Referring to Fig. 8, shown is a method for authenticating a user, the user having enrolled previously as described *supra*. In use, the user wishing to be authenticated, for instance to gain access to one of a secure location and a secure data file, places at step

**130** a predetermined fingertip **51** onto the sensing area **52** of the fingerprint scanner **53**. Optionally, for instance if the user provided a plurality of different fingertips during the enrollment process, the user selects a fingertip at random or selects a fingertip in response to a prompt by the system **50**. At step **131** the ridge-and-valley pattern of the fingertip **51** is sensed electronically by the sensing area **52** and an image of the fingerprint is captured by the fingerprint scanner **53**. The fingerprint image is provided to the processor **54**, processed by the processor **54** to clean up the image, and stored in the second area **55b**. Optionally, the fingerprint image is stored directly as captured by the fingerprint scanner **53** and is retrieved by the processor **54**.

[0081] At step **132** the fingerprint image is processed using code in execution on the processor **54** to determine a value indicative of a characteristic, such as for instance a moisture level condition, of the fingerprint. For example, image processing is employed to quantify the incidences of fingerprint ridge discontinuities and interconnects, and to compare a result of said quantification with a database of expected values for different fingerprint moisture levels. The determined value indicative of a moisture level of the fingerprint is a relative score, wherein 'dry' or 'very dry' are at one extreme and 'moist' or 'very moist' are at the other extreme. In dependence upon the determined value indicative of a moisture level of the fingerprint, the processor **54** selects at step **133** an authorized fingerprint template image obtained under similar moisture level conditions and retrieves same from the first memory area **55a**.

[0082] At step **134** the processor **54** compares the fingerprint image with the selected authorized fingerprint template image. For instance, the processor extracts features or minutiae of the image for comparison with similar extracted features or minutiae of the selected authorized fingerprint template image according to processes that are well known to those of skill in the art. If at decision step **135** the result of the comparison indicates a match between the fingerprint image and the selected authorized fingerprint template image, the user at step **136** is authenticated by the system **51** and the method of Fig. 8 terminates at step **137**. If at decision step **135** the result of the comparison indicates other than a match between the fingerprint image and the selected authorized fingerprint template image, the availability of other similar template images is determined

at optional step **138**. If other similar template images are available, a second authorized fingerprint template image is selected at optional step **139**, and steps **134** and **135** are repeated. If it is determined at optional step **138** that other similar template images are other than available, the user is rejected at step **140** and the method of Fig. 8 terminates at step **137**.

[0083] Optionally, at step **134** a predetermined process is used to 'clean-up' the fingerprint image, for instance all ridge discontinuities and ridge interconnects are digitally removed, smoothed and/or otherwise processed to produce a processed fingerprint image. The processed fingerprint image is compared to a similarly processed template image, which template image was stored in association with a same moisture level condition of the original fingerprint image.

[0084] Referring to Fig. 9, shown is another method for authenticating a user, the user having enrolled previously as described *supra*. In use, the user wishing to be authenticated, for instance to gain access to one of a secure location and a secure data file, places at step **130** a predetermined fingertip **51** onto the sensing area **52** of the fingerprint scanner **53**. Optionally, for instance if the user provided a plurality of different fingertips during the enrollment process, the user selects a fingertip at random or selects a fingertip in response to a prompt by the system **50**. At step **131** the ridge-and-valley pattern of the fingertip **51** is sensed electronically by the sensing area **52** and an image of the fingerprint is captured by the fingerprint scanner **53**. The fingerprint image is provided to the processor **54**, processed by the processor **54** to clean-up the image, and stored in the second area **55b**. Optionally, the fingerprint image is stored directly as captured by the fingerprint scanner **53** and is retrieved by the processor **54**.

[0085] At step **132** the fingerprint image is processed using code in execution on the processor **54** to determine a value indicative of a characteristic, such as for example a moisture level, of the fingerprint. For instance, image processing is performed to quantify the incidences of fingerprint ridge discontinuities and interconnects, and to compare a result of said quantification with a database of expected values for different fingerprint moisture levels. The determined value indicative of a moisture level of the

fingerprint is a relative score, wherein 'dry' or 'very dry' are at one extreme and 'moist' or 'very moist' are at the other extreme. In dependence upon the determined value indicative of the characteristic of the fingerprint, the processor 54 selects at step 141 a process for processing the fingerprint. If the characteristic of the fingerprint is indicative of the fingertip being dry, then a selected process removes at step 142 all of the ridge discontinuities in the image. Similarly, if the characteristic of the fingerprint is indicative of the fingertip being moist, then a second different selected process removes at step 142 all of the ridge interconnections. Of course, if the characteristic of the fingerprint is indicative of the fingertip being normal, then a third different selected process at step 142 performs only a general clean-up of the captured image.

[0086] At step 143 the processed fingerprint image is compared to at least a template image to perform one of an identification operation and a verification operation, such as to authenticate the user. If at decision step 144 a match is indicated, the user is authenticated at step 136. Of course, if other than a match is indicated at decision step 144, the user is rejected at step 136.

[0087] The method of Fig. 9 terminates at step 137.

[0088] Advantageously, only the ridge discontinuities are removed from a 'dry' fingerprint image, such that the image so processed retains actual ridge interconnect features, which features are useful for confirming the identity of the user. Similarly, only the ridge interconnects are removed from a 'moist' fingerprint image, such that the image so processed retains actual ridge discontinuity features, which features are also useful for confirming the identity of the user. As such, selecting the image-processing process in dependence upon the determined characteristic of the fingerprint provides a larger set of extractable features for use with the authentication method according to Fig. 9.

[0089] Referring to Fig. 10, shown is another method for authenticating a user, the user having been enrolled previously as described *supra*. The method according to Fig. 10 is intended for with a system to perform a one-to-one identification of a user. The user at step 145 provides their identity and places a predetermined fingertip 51 onto the sensing area 52 of the fingerprint scanner 53. Optionally, for instance if the user provided a

plurality of different fingertips during the enrollment process, the user selects a fingertip at random or selects a fingertip in response to a prompt by the system 50. At step 146 the ridge-and-valley pattern of the fingertip 51 is sensed electronically by the sensing area 52 and an image of the fingerprint is captured by the fingerprint scanner 53. The fingerprint image is provided to the processor 54, processed by the processor 54 to clean-up the image, and stored in the second area 55b. Optionally, the fingerprint image is stored directly as captured by the fingerprint scanner 53 and is retrieved by the processor 54.

[0090] At step 147 the fingerprint image is processed using code in execution on the processor 54 to determine a value indicative of a characteristic, such as for example a moisture level, of the fingerprint. For instance, image processing is performed to quantify the incidences of fingerprint ridge discontinuities and interconnects, and to compare a result of said quantification with a database of expected values for different fingerprint moisture levels. The determined value indicative of a moisture level of the fingerprint is a relative score, wherein 'dry' or 'very dry' are at one extreme and 'moist' or 'very moist' are at the other extreme. In dependence upon the determined value indicative of the characteristic of the fingerprint, the processor 54 selects at step 148 a process for processing the fingerprint.

[0091] At step 149 a fingerprint template associated with the identity provided by the user at step 145 is retrieved from memory storage. At step 150 the fingerprint image and the retrieved template image are processed separately according to the process selected at step 148. If the characteristic of the fingerprint determined at step 147 is indicative of the fingertip being dry, then a selected process removes at step 150 all of the ridge discontinuities in the image. Similarly, if the characteristic of the fingerprint determined at step 147 is indicative of the fingertip being moist, then a second different selected process removes at step 150 all of the ridge interconnections. Of course, if the characteristic of the fingerprint determined at step 147 is indicative of the fingertip being normal, then a third different selected process at step 150 performs only a general clean-up of the captured image.

FIG. 10



[0092] Preferably, each process includes code for filtering the template image to determine features that are unique to the user that provided said template image. Such features include: ridge discontinuities, ridge interconnects, scars, wrinkles etc. Advantageously, permanent features identified in the template and located within the fingerprint image during processing thereof are other than removed from the fingerprint image. This is particularly significant when the permanent features appear otherwise to be a moisture-dependent transient feature of the fingerprint.

[0093] At step 151 the processed fingerprint image is compared to the processed template image to perform one of an identification operation and a verification operation, such as to authenticate the user. If at decision step 152 a match is indicated, the user is authenticated at step 136. Of course, if other than a match is indicated at decision step 152, the user is rejected at step 136.

[0094] The method of Fig. 10 terminates at step 137.

[0095] Of course, the fingerprint scanner 53 for scanning template images during the enrollment process of Figs. 7a-7d is located optionally in a secure location to control access thereto. Other fingerprint scanners, which are located at remote locations and/or are integrally formed into electronic devices, walls, doors or furniture, are provided for identifying and/or verifying users requesting authentication at said remote locations. Optionally, the other fingerprint scanners are lower resolution, and thus relatively inexpensive, compared to the centrally located enrollment scanner. Of course, each of the other fingerprint scanners is in electrical communication with the processor 54. Optionally, each of the other fingerprint scanners comprises a separate processor, each separate processor in electrical communication with the memory storage device 55, which is within a central, secure location.

[0096] Numerous other embodiments may be envisaged without departing from the spirit and scope of the invention.